IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Brian Jacoby et al. Art Unit : 2143
Serial No. : 09/894,918 Examiner : Alina Boutah
Filed : June 29, 2001 Confirmation No.: 5947
Title : DEEP PACKET SCAN HACKER IDENTIFICATION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

# APPENDIX

Amendments to the Claims **(with true markings for the May 3, 2006 response that includes underlines, brackets, and strike through format)**:

Listing of Claims:

1. (Currently amended) A method for securing an accessible computer system, the method comprising:

receiving more than one data packet at a network device, each data packet including a payload portion and an attribute portion and being communicated between at least one access requestor and at least one access provider through the network device;

monitoring, at the network device, at least the payload portion of the data packets directed from at least one of the access providers to at least one of the access requestors by scanning the payload portion for at least one predetermined pattern and counting a number of data packets having payload portions that include the predetermined pattern; and

using the network device to denying communication of subsequent ~~access by~~ data packets from the access requestor to the access provider when a number of payload portions of the data packets received from the access provider to the access requestor are deemed to include the predetermined pattern exceed a configurable threshold number.

2. (Canceled).

3. (Currently amended) The method as in claim 1 wherein monitoring the data packets includes scanning the payload portion while handling the data packets with a ~~switch~~ network device.

4. (Previously presented) The method as in claim 3 wherein

monitoring the data packet includes monitoring only at least one data packet that is distinguished.

5. (Previously presented) The method as in claim 1 wherein:

securing the accessible computer system further comprises distinguishing at least one of the data packets from among the data packets received for additional processing, and

monitoring the payload portion includes monitoring the payload portion of the at least one data packet distinguished.

6. (Original) The method as in claim 5 wherein the at least one data packet is distinguished based on an Internet address associated with the data packet.

7. (Previously presented) The method as in claim 1 wherein

monitoring the data packet includes monitoring all of the data packets received.

8. (Canceled).

9. (Canceled).

10. (Canceled).

11. (Previously presented) The method as in claim 1 wherein the predetermined pattern includes a login failure message communicated from the access provider to the access requestor.

12. (Previously presented) The method as in claim 1 wherein the data packets include a token-based protocol packet, or a TCP packet or a PPP packet.

13-15. (Canceled).

16. (Currently amended) The method as in claim 1 wherein denying communication of subsequent ~~access~~data packets includes affecting bandwidth for communications between the access requestor and the access provider.

17. (Previously presented) The method as in claim 1 further comprising rerouting the access requestor.

18. (Canceled).

19. (Currently amended) The method as in claim 1 wherein denying subsequent ~~access by~~ data packets from the access requestor to the access provider includes denying ~~access by~~ data packets from the access requestor to the access provider when a number of payload portions that include the predetermined pattern exceed a configurable threshold number during a configurable period of time.

20. (Currently amended) A system that connects a plurality of access requestors to a plurality of access providers for securing an accessible computer system, comprising:

a receiving component that is structured and arranged to receive more than one data packet, each data packet including a payload portion and an attribute portion and being communicated between at least one access requestor and at least one access provider;

a monitoring component that is structured and arranged to monitor at least the payload portion of the data packets directed from at least one of the access providers to at least one of the access requestors and includes a scanning component that is structured and arranged to scan the payload portion for at least one predetermined pattern and to count a number of data packets having payload portions that include the predetermined pattern; and

an access controlling component that is structured and arranged to deny communication of subsequent ~~access by~~ data packets from the access requestor to the access provider when a number of payload portions of data packets received from the access provider to the access requestor that include the predetermined pattern exceed a configurable threshold number.

21. (Canceled).

22. (Currently amended) The system of claim 20 wherein the monitoring component includes a scanning component that is structured and arranged to scan the payload portion while handling the data packets with a ~~switch~~ network device.

23. (Previously presented) The system of claim 22 wherein

the monitoring component is structured and arranged to monitor only at least one data packet that is distinguished.

24. (Previously presented) The system of claim 20 wherein:

the system further comprises a distinguishing component that is structured and arranged to distinguish at least one of the data packets from among the data packets received for additional processing, and

the monitoring component is structured and arranged to monitor the payload portion of the at least one data packet distinguished.

25. (Original) The system of claim 24 wherein the at least one data packet is distinguished based on an Internet address associated with the data packet.

26. (Previously presented) The system of claim 20 wherein

the monitoring component is structured and arranged to monitor all of the data packets received.

27. (Canceled).

28. (Previously presented) The system of claim 20 wherein the data packets are monitored when communicated from the access requestor to the access provider.

29. (Canceled).

30. (Previously presented) The system of claim 20 wherein the predetermined pattern includes a login failure message communicated from the access provider to the access requestor.

31. (Previously presented) The system of claim 20 wherein the data packets include a token-based protocol packet, or a TCP packet or a PPP packet.

32 - 34. (Canceled).

35. (Original) The system of claim 20 wherein the access controlling component is structured and arranged to affect bandwidth for communications between the access requestor and the access provider.

36. (Original) The system of claim 20 wherein the access controlling component is structured and arranged to reroute the access requestor.

37. (Canceled).

38. (Previously presented) The system of claim 20 wherein the access controlling component is structured and arranged to deny subsequent access by the access requestor to the access provider when a number of payload portions that include the predetermined pattern exceed a configurable threshold number during a configurable period of time.

39. (Currently amended) A computer program stored on a network device computer that connects a plurality of access requestors to a plurality of access providers ~~readable medium or a propagated signal~~ for securing an accessible computer system, comprising:

a receiving code segment that causes the computer to receive more than one data packet, each data packet including a payload portion and an attribute portion and being communicated between at least one access requestor and at least one access provider;

a monitoring code segment that causes the computer to monitor at least the payload portion of the data packets directed from at least one of the access providers to at least one of the access requestors and includes a scanning code segment that causes the computer to scan the payload portion for at least one predetermined pattern and to count a number of data packets having payload portions that include the predetermined pattern; and

an access controlling code segment that causes the computer to deny subsequent communication of ~~access by~~ data packets from the access requestor to the access provider when a number of payload portions of the data packets received from the access provider to the access requestor that include the predetermined pattern exceed a configurable threshold number.

40. (Canceled).

41. (Currently amended) The computer program of claim 39 wherein the monitoring code segment includes a scanning code segment that causes the computer to scan the payload portion while handling the data packets with a ~~switch~~ network device.

42. (Previously presented) The computer program of claim 41 wherein

the monitoring code segment causes the computer to monitor only at least one data packet that is distinguished.

43. (Previously presented) The computer program of claim 39 wherein:

the computer program further comprises a distinguishing code segment that causes the computer to distinguish at least one of the data packets from among the data packets received for additional processing, and

the monitoring code segment causes the computer to monitor the payload portion of the at least one data packet distinguished.

44. (Original) The computer program of claim 43 wherein the at least one data packet is distinguished based on an Internet address associated with the data packet.

45. (Previously presented) The computer program of claim 39 wherein

the monitoring code segment causes the computer to monitor all of the data packets received.

46. (Canceled).

47. (Previously presented) The computer program of claim 39 wherein the data packets are monitored when communicated from the access requestor to the access provider.

48. (Canceled).

49. (Previously presented) The computer program of claim 39 wherein the predetermined pattern includes a login failure message communicated from the access provider to the access requestor.

50. (Previously presented) The computer program of claim 39 wherein the data packets include a token-based protocol packet, or a TCP packet or a PPP packet.

51 - 53. (Canceled).

54. (Original) The computer program of claim 39 wherein the access controlling code segment causes the computer to affect bandwidth for communications between the access requestor and the access provider.

55. (Original) The computer program of claim 39 wherein the access controlling code segment causes the computer to reroute the access requestor.

56. (Canceled).

57. (Previously presented) The computer program of claim 39 wherein the access controlling code segment causes the computer to deny subsequent access by the access requestor to the access provider when a number of payload portions that include the predetermined pattern exceed a configurable threshold number during a configurable period of time.

58. (Currently amended) The method as in claim 1 wherein denying communication of subsequent ~~access by~~ data packets from the access requestor to the access provider further comprises denying communication of subsequent ~~access~~ data packets from a group of access requestors to the access provider when a number of payload portions within the data packets that are received, from the access provider by at least one access requester which is a group member, include the predetermined pattern exceed a configurable threshold number.

59. (Previously presented) The method of claim 1 further comprises determining whether the access requestor is on a permitted access list that is associated with the access requestors allowing subsequent access from the access requestor to the access provider conditioned on whether or not the access requestor is determined to be included in the permitted access list.

60. (Previously presented) The method of claim 59 wherein determining whether the access requestor is included in the permitted access list further comprises determining whether the IP address of the access requestor is included in the permitted access list.

61. (Currently amended) The method of claim 1 wherein subsequent ~~access by~~ data packets from the access requestor to the access provider is denied for a pre-determined and limited period of time.

62. (Currently amended) The method of claim 61 wherein denial of subsequent ~~access by~~ data packets from by the access provider starts a new pre-determined and limited time period upon detecting an access request the access requestor during the elapsing of the predetermined and limited period of time.

63. (Cancelled).

64. (Currently amended) The method of claim 1 wherein denying subsequent ~~access by~~ data packets from the access requestor is performed in response to a command received from the access provider, irrespective of the inspection of data packets received from the access provider.

65-66. (Cancelled).

[[68]]67. (Currently amended) The method of claim 11 wherein the predetermined pattern further includes a login request message.

[[69]]68. (Currently amended) The method of claim 11 wherein the login failure message includes a signature located at a specific offset from an end of the data packet communicated from the access provider to the access requestor.

[[70]]69. (Currently amended) The method of clam 11 wherein the login failure message includes login failure reasons.

70. (New) The method of claim 1 wherein the network device is a physically independent processor from the access providers.